UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/487,946	01/19/2000	Bjorn Markus Jakobsson	Jakobsson 13-1	3763

27550 7590 07/21/2004

WALTER J, TENCZA JR.
10 STATION PLACE, SUITE 3
METUCHEN, NJ 08840

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 07/21/2004

13

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/487,946	Applicant(s) JAKOBSSON ET AL.	
	Examiner Jung W Kim	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 May 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5-11 and 13-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5-11 and 13-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 2, 5-11 and 13-18 have been examined. Applicant has amended claims 1, 2, 5, 6, 8, 11, 13 and 14, and added new claims 15-18.

Response to Amendment

2. The 35 U.S.C. 112, 1st paragraph rejections to claims 1-2, 5-11, and 13-14 are withdrawn as the amendments to the independent claims overcome the rejections.

3. The 35 U.S.C. 112, 2nd paragraph rejections to claims 1, 6, 8, and 11 are withdrawn as the amendments to the claims overcome the rejections.

Response to Arguments

4. In view of the amendments to claims 1, 2, 5-11 and 13-18, a new ground(s) of rejection is made under 35 U.S.C. 103(a).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 2, 5, 9-11, 13, 14, 15 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier Applied Cryptography 2nd Edition (hereinafter Schneier) in view of Deo U.S. Patent No. 5,721,781 (hereinafter Deo). As per claim 1, Schneier teaches an ElGamal encryption method which substantially covers the claim (see Schneier, page 478, 'ElGamal Encryption'). Although the method disclosed by Schneier in this section does not expressly disclose encrypting a key value (the ElGamal scheme is taught as a method to encrypt a general message), it is conventional in the art to use public key encryption methods for secure key exchange (see Schneier, pages 518-522, especially page 519, 'Implementing EKE with ElGamal'). Further, message encryption is typically divided into two work loads: a public key encryption method used to exchange a session key and a symmetric algorithm using this session key to encrypt the message (see Schneier, page 216, 'Public-Key Cryptography verses Symmetric Cryptography'; pages 518-522, section 22.5 'Encrypted Key Exchange'). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to use the ElGamal encryption method as disclosed by Schneier to securely transmit a secret key from a sender to a receiver for the purpose of encrypting and decrypting a message with the secret key. Motivation for such a combination would enable a faster cryptosystem for the secure transmission of messages as taught by Schneier. Hence, the ElGamal encryption method comprises the steps of:

a. encrypting a message M using a primary secret key z to form a quantity E;

b. encrypting a session key z by preparing:

i. a(new) = z*y^c modulo p;

ii. b(new) = g^c modulo p;

where y = g^x modulo p, c is a random number, x is a receiver secret key, and the parameters g, x, and p are picked using a known encryption method;

c. decrypting a(new) and b(new) using the receiver secret key x to get the primary secret key z;

d. using the primary secret key z to decrypt the quantity E and obtain M (see Schneier, pages 478, 'ElGamal Encryption'; pages 513-515, 'Diffie-Hellman').

7. This encryption method disclosed by Schneier does not specify the step of generating a signature based on the triplet a(new), b(new) and E. However, as disclosed by Schneier in a separate section, signing documents is the standard methodology to ensure the identity of the author of a message and to verify the integrity of the message (see Schneier, pages 34-44, 'Digital Signatures', 'Digital Signatures with Encryption'). It would be obvious to one of ordinary skill in the art at the time the invention was made to generate a signature s(new) as a function of a(new), b(new), and E by the sender and have the receiver of the transmission validate the signature. Motivation for such a combination would enable the invention to implement a more secure transmission methodology by authenticating the author of the transmission and verifying the integrity of the transmission as taught by Schneier. Finally, Schneier is silent on the matter of the same random number c being used in the key encryption step and in the signature step. However, this step would be an obvious construction for a plurality of reasons: 1) the number of random numbers generated for an iteration of the

method is reduced and thereby improve the efficiency of the method; 2) fewer secret values equate to fewer opportunities for exposure; and 3) minimization of the number of random numbers used enables the random number generator to generate random numbers without duplicating the values for a longer period of time, since random number generators are periodic (random numbers created by a random number generator are predefined as having a lower and upper bound) (see Schneier, page 44, 4th full paragraph, last 4 sentences). Furthermore, security of these different method steps is commonly maintained by securing the key encryption and signature implementations together. This type of implementation is typical since it places all sensitive steps in one tamperproof secure device. One example is a smart card implementing both an encryption step and a signature step as taught by Deo (see Deo, col. 7, lines 10-34). It would be obvious to one of ordinary skill in the art at the time the invention was made to use the same random number c in both the key encryption step and the signature step when both steps are secured together. Motivation for such an implementation enables the method to reduce the number of random numbers needed for operation of the secure method for the reasons outlined above. The aforementioned covers claim 1.

8. As per claim 2, Schneier covers an ElGamal encryption method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the step of decrypting a(new) and b(new) using the receiver secret key x to get the primary

transmitter secret key z is comprised of computing z = a(new)/b(new)^x (see Schneier, page 478, 'ElGamal Encryption').

9. As per claim 5, Schneier covers an ElGamal encryption method as outlined above in the claim 2 rejection under 35 U.S.C. 103(a). Schneier is silent on the matter of defining a function to determine the value of z. However, the members of the set Z = {g^k modulo p | k is a nonnegative number} are obvious candidates since this set would enable the value z*y^c modulo p to be a member of the group G modulo p generated by the generator g of order @(p), where g and p are relatively prime, @() is Euler's totient function, and g^@(p) = 1 modulo p. Since:

z*y^c modulo p = (g^k modulo p * g^(x*c) modulo p) modulo p

= g^(k+x*c) modulo p.

a(new) is a one to one function of k given that 0 <= k+x*c <= @(p), where x and c are held constant. Hence, using the aforementioned constraints, the sender can be confident that distinct values of k will generate distinct primary transmitter secret keys z. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to generate the primary transmitter secret key from the formula z = g^k modulo p, where k is a random value chosen from the set [0...q], where q is a value picked using a known encryption method.

10. As per claims 9 and 10, Schneier covers an ElGamal encryption method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, in different

sections, Schneier teaches two standard methods to sign messages that have shown to be effective as digital signatures: Schnorr signature method and Digital Signature Standard (see Schneier, pages 510-512, 'Schnorr'; pages 483-494, 'Digital Signature Algorithm'). It would be obvious to one of ordinary skill in the art at the time the invention was made to create the signature using either the Schnorr signature method or the DSS method since both are proven standards as taught by Schneier.

11. As per claims 11 and 13-14, Schneier covers an ElGamal encryption method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, a processor is used to implement the steps defined in the claims 1, 9, and 10 as covered by the invention taught by Schneier and modified by Deo (see Deo, Figure 1).

12. As per claims 15 and 18, Schneier covers an ElGamal encryption method/apparatus as outlined above in the claim 1 and 11 rejections under 35 U.S.C. 103(a). In addition, as mentioned above, Schneier teaches ElGamal encryption means used for encrypting messages (see Schneier, pages 478, 'ElGamal Encryption'). It would be obvious to one of ordinary skill in the art at the time the invention was made to encrypt the data message with an ElGamal encryption scheme, since it is a secure encryption scheme that is not patented, and hence, requires no license to be used as taught by Schneier (see Schneier, page 479, 'Patents').

13. Claims 6, 7, 8, 16, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Deo as applied to claim 1 above, and further in view of admitted prior art as disclosed by the applicant in the specification (hereinafter admission). As per claims 6 and 7, Schneier covers an ElGamal encryption method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Schneier is silent on the matter of defining 2 private transmitter keys z and z' where z' = f(z) for some function f() and z' is the key which encrypts and decrypts the message M. However, as disclosed by admission, it is conventional in the art to use functions, such as truncation, to modify a generated key value to be used in an encryption method that requires a different key length (see admission, page 12, line 14 – page 13, line 3). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to define a second private transmitter key z', where z' = f(z) for some function f() and z' is the key used to encrypt and decrypt the message M, when the primary transmitter key z is provided and is not of the format used for producing the ciphertext E. The motivation for such an implementation would enable the invention disclosed by Schneier to implement a function to encrypt message M that is independent (or at least less dependent) of the function that generated the first primary transmitter key z. This independence enables the cryptosystem to be designed with functions based more on security benefits than on compatibility issues.

14. As per claim 8, Schneier covers an ElGamal encryption method as outlined above in the claim 7 rejection under 35 U.S.C. 103(a). In addition, admission discloses

providing a plurality of portion keys which are derived from the secondary transmitter key z' and the plurality of portion keys encrypts and decrypts a data message m when the secondary transmitter key z' is provided which is not of the format used for producing the ciphertext E (see admission, page 12, line 14 – page 13, line 3).

15. As per claims 16 and 17, they are method claims corresponding to claims 6, 8, 15 and 18, and they do not teach or define above the information claimed in claims 6, 8, 15, and 18. Therefore, claims 16 and 17 are rejected as being unpatentable over Schneier in view of Deo and admission for the same reasons set forth in the rejections of claims 6, 8, 15, and 18.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
July 6, 2004

JUSTIN T. DARROW
PRIMARY EXAMINER